

Beschreibung

Einräumung eines Zugriffs auf ein computerbasiertes Objekt

- 5 Die vorliegende Erfindung betrifft ein Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt und ein Steuerungsprogramm zur Durchführung des Verfahrens.

- 10 Durch unberechtigte Benutzung von Computerprogrammen entstehen weltweit immense Schäden. Um diesem entgegenzuwirken, werden Lösungen zum Schutz von Computerprogrammen vor unberechtigter Benutzung entwickelt.

- 15 Eine Übermittlung verschlüsselter Informationen zur Aktivierung eines Computerprogramms dient einer Verhinderung von nicht autorisierten Vervielfältigungen des Computerprogramms. Entsprechende Verfahren dienen beispielsweise außerdem als technische Voraussetzung, um Computerprogramme als Produkte über E-Commerce zu vertreiben. Bei bisher bekannten Verfahren
- 20 zur Aktivierung von Computerprogrammen werden Computerprogramme anhand jeweils eines Registrierungsschlüssels freigeschaltet. Für eine Freischaltung eines Computerprogramms wird der Registrierungsschlüssel, der einer Computerprogrammlizenz fest zugeordnet ist, manuell eingegeben bzw. von einem Daten-
- 25 träger eingespielt. Insbesondere bei einer Vielzahl von auf unterschiedlichen Computern installierten Computerprogrammen resultiert hieraus ein hoher Administrationsaufwand, der mit personalintensiven Bedien- und Wartungsarbeiten verbunden ist.

30

- Aus EP 1 191 419 A2 ist Verfahren bekannt, bei dem vorgebbare Funktionen eines Computerprogramms für eine wählbare Nutzungsdauer durch Modifikation eines Registrierungsschlüsselpaares freigeschaltet werden können. Das Registrierungs-
- 35 schlüsselpaars weist zumindest eine gegenüber Benutzerzugriffen gesperrten Teilinformation auf. Die freizuschaltenden Funktionen müssen nicht notwendigerweise bereits bei ei-

ner Erstinstallation des Computerprogramms für eine Freischaltung zur Verfügung gestanden haben, sondern können auch nachträglich hinzugewählt werden. Zur Freischaltung ist kein Einsatz von Bedien- und Wartungspersonal am Ort des Computers erforderlich, auf der das jeweilige Computerprogramm installiert ist.

Bestandteile des Registrierungsschlüsselpaares entsprechend dem in EP 1 191 419 A2 beschriebenen Verfahren sind Applikationsinformationen und ein Applikationswert. Die Applikationsinformationen werden an einem ersten Computer eingegeben, auf der das zu registrierende Computerprogramm installiert ist, bzw. durch den ersten Computer generiert. Der Applikationswert wird in einem zweiten Computer mittels Codierung aus den Applikationsinformationen berechnet.

Bei einer Registrierung eines Computerprogramms oder einer Änderung der Registrierung werden erste Applikationsinformationen mit zumindest einer gegenüber Benutzerzugriffen gesperrten Teilinformation an den zweiten Computer übermittelt. Im zweiten Computer wird aus den ersten Applikationsinformationen ein Applikationswert berechnet, der nachfolgend an den ersten Computer übermittelt wird. Mittels Decodierung werden im ersten Computer aus dem Applikationswert zweite Applikationsinformationen ermittelt. Die ersten und die zweiten Applikationsinformationen werden bei einem Ausführungsbeginn des Computerprogramms auf Übereinstimmung überprüft. In Abhängigkeit der sich bei der Überprüfung ergebenden Abweichungen werden vorgebbare Funktionen des Computerprogramms freigeschaltet.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde ein Verfahren, das einen erhöhten Schutz vor unberechtigter Benutzung von in einer Recheneinrichtung bereitgestellten Ressourcen bietet, sowie eine zur automatisierten Durchführung des Verfahrens geeignete Implementierung anzugeben.

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren mit den in Anspruch 1 und ein Steuerungsprogramm mit den in Anspruch 10 angegebenen Merkmalen gelöst. Vorteilhafte Ausgestaltungen der vorliegenden Erfindung sind in den abhängigen Ansprüchen angegeben.

Erfindungsgemäß resultiert ein erhöhter Schutz vor unberechtigter Benutzung von in einer Recheneinrichtung bereitgestellten Ressourcen daraus, daß als eine Voraussetzung zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt eine Speicherkarte mit einem Programmcodeprozessor und eine Lizenzinformation bereitgestellt werden. Auf der Speicherkarte sind zumindest ein der Speicherkarte zugeordneter öffentlicher und privater Schlüssel sowie ein öffentlicher Schlüssel einer vertrauenswürdigen Instanz abgespeichert. Die Lizenzinformation umfaßt zumindest einen mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode und wird an einer den Zugriff auf das computerbasierte Objekt steuernden Recheneinrichtung bereitgestellt. Der verschlüsselte Lizenzcode und eine mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes werden an die Speicherkarte übermittelt. Die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion wird nachfolgend überprüft. Bei positivem Überprüfungsergebnis wird die Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte ausgeführt und ein entschlüsselter Lizenzcode an die Recheneinrichtung übermittelt. Der entschlüsselte Lizenzcode wird dann zumindest temporär zum Zugriff auf das computerbasierte Objekt bereitgestellt.

Unter Recheneinrichtung sind beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs PCs, Notebooks, Server, PDAs, Mobiltelefone, Geldautomaten, Steuerungsmodule in der Automatisierungs-, Fahrzeug-, Kommunikations- oder Medizintechnik zu verstehen - allgemein Einrichtungen, in denen Com-

puterprogramme ablaufen können. Des weiteren sind computerbasierte Objekte beispielsweise ohne Beschränkung der Allgemeinheit dieses Begriffs Betriebssysteme, Steuerungs- oder Anwendungsprogramme, durch Betriebssysteme, Steuerungs- oder
5 Anwendungsprogramme bereitgestellte Dienste, Leistungsmerkmale, Funktionen oder Prozeduren, Zugriffsrechte auf Peripheriegeräte sowie auf einem Speichermedium befindliche Daten.

Entsprechend einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird der öffentliche Schlüssel der vertrauenswürdigen Instanz vor Manipulationen geschützt an der Recheneinrichtung bereitgestellt. Außerdem ist die Lizenzinformation mittels eines privaten Schlüssels der vertrauenswürdigen Instanz digital signiert. Die digitale Signatur der Lizenzinformation kann somit in der Recheneinrichtung anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft werden. Auf diese Weise kann eine vertrauenswürdige und sichere Übermittlung der Lizenzinformation zur Recheneinrichtung gewährleistet werden.

20 Vorteilhafterweise umfaßt die Lizenzinformation zusätzlich den der Speicherkarte zugeordneten öffentlichen Schlüssel. Des weiteren wird der entschlüsselte Lizenzcode mittels des der Speicherkarte zugeordneten privaten Schlüssels digital
25 signiert. Die digitale Signatur des entschlüsselten Lizenzcodes kann dann in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels überprüft werden. Dies bietet den Vorteil einer gesicherten Übertragung des entschlüsselten Lizenzcodes an die Recheneinrichtung,
30 verbunden mit der Sicherstellung, daß der Lizenzcode tatsächlich mit der zur Entschlüsselung vorgesehenen Speicherkarte entschlüsselt worden ist.

Darüber hinaus kann die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe der von
35 der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes in der Recheneinrichtung aus dem verschlüs-

seltem Lizenzcode und einem Signatur-Objekt erzeugt werden. Das Signatur-Objekt umfaßt nur einen Signaturanteil eines von der vertrauenswürdigen Instanz signierten Funktionsaufrufs zur Entschlüsselung des Lizenzcodes. Diese Ausgestaltung bietet den Vorteil, daß verfügbare Secure-Messaging-Verfahren für eine Übermittlung eines entsprechenden Funktionsaufrufs verwendet werden können. Ferner kann die Lizenzinformation zusätzlich das Signatur-Objekt umfassen, so daß eine gesicherte Bereitstellung des Signatur-Objektes gewährleistet werden kann.

Entsprechend einer weiteren vorteilhaften Ausgestaltung der vorliegenden Erfindung werden der verschlüsselte Lizenzcode und die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt. Hierdurch werden Manipulationsmöglichkeiten zur unberechtigten Erlangung des Zugriffs auf das computerbasierte Objekt weiter eingeschränkt.

Vorteilhafterweise wird die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft. Dies dient einer Verhinderung einer unberechtigten Entschlüsselung des Lizenzcodes.

Gemäß einer weiteren Ausgestaltung der vorliegenden Erfindung wird in der Recheneinrichtung eine Zufallszahl erzeugt und diese an die Speicherkarte übermittelt. Der entschlüsselte Lizenzcode wird dann mittels des der Speicherkarte zugeordneten privaten Schlüssels und der Zufallszahl digital signiert. Die digitale Signatur des entschlüsselten Lizenzcodes wird schließlich in der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels und der Zufallszahl überprüft. Hierdurch ergibt sich ein wirksamer Wiederho-

lungsschutz, so daß ein Abfangen von zwischen der Speicherkarte und der Recheneinrichtung ausgetauschten Signalen keine wirksamen Manipulationsmöglichkeiten eröffnet.

5 Entsprechend einer bevorzugten Ausgestaltung der vorliegenden Erfindung werden zur Einräumung des Zugriffs auf das computerbasierte Objekt der entschlüsselte Lizenzcode und ein Überprüfungsprozeßverlauf mit einer jeweiligen Soll-Vorgabe abgeglichen. Dies bietet zusätzliche Sicherheit, da ein Vor-
10 liegen des entschlüsselten Lizenzcodes für eine Zugriffsberechtigung alleine nicht mehr ausreichend ist, sondern an einen erfolgreichen Überprüfungsprozeßverlauf gekoppelt ist.

Die vorliegende Erfindung wird nachfolgend an einem Ausführungsbeispiel anhand der Zeichnung näher erläutert.
15

Es zeigt die Figur eine schematische Darstellung eines Anwendungsumfeldes der vorliegenden Erfindung mit einem Informations- und Meldungs austausch zwischen einer vertrauenswürdigen
20 Instanz, einer den Zugriff auf ein computerbasiertes Objekt steuernden Recheneinrichtung und einer Speicherkarte mit Programmcodeprozessor.

Das in der Figur dargestellte Anwendungsumfeld der vorliegenden Erfindung umfaßt eine vertrauenswürdige Instanz 10, einen
25 Computer 20, ein mit dem Computer 20 verbundenes Smartcard-Terminal 30, in das eine Smartcard 40 einführbar ist. Die vertrauenswürdige Instanz 10 kann beispielsweise einem Hersteller einer gegen unberechtigten Zugriff zu schützenden
30 Software zugeordnet sein und übernimmt eine Verwaltung von Lizenzen und zu Smartcard zugeordnetem Schlüsselmaterial. Der vertrauenswürdigen Instanz 10 ist ferner ein asymmetrisches Schlüsselpaar 11 zugeordnet, daß einen privaten und einen öffentlichen Schlüssel umfaßt. Zur Abspeicherung des zu Smart-
35 card zugeordnetem Schlüsselmaterial ist eine Datenbasis 12 vorgesehen, welche öffentliche Schlüssel auszuliefernder bzw. bereits ausgelieferter Smartcards enthält.

- Durch den Computer 20 werden für einen oder mehrere Benutzer Systemressourcen 22 verfügbar gemacht, die beispielsweise Programme oder Speicherbereiche mit Daten umfassen. Das hier
- 5 beschriebene Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt ist grundsätzlich auf beliebige Systemressourcen anwendbar. Der Computer 20 steuert insbesondere einen Zugriff auf die Systemressourcen 22, die im vorliegenden Fall auch Software des Herstellers umfassen, welchem die
- 10 vertrauenswürdige Instanz 10 zugeordnet ist. Des weiteren wird der öffentliche Schlüssel 21 der vertrauenswürdigen Instanz 10 vor Manipulation geschützt am Computer 20 bereitgestellt.
- 15 Mit dem Computer 20 ist das Smartcard-Terminal 30 über eine gesicherte Kommunikationsverbindung verbunden. Das Smartcard-Terminal 30 dient zum Informations- und Meldungs austausch zwischen dem Computer 20 und einer in das Smartcard-Terminal 30 einführbaren Smartcard 40, die eine Speicherkarte mit ei-
- 20 nem Programmcodeprozessor darstellt. Auf der Smartcard 40 ist der öffentliche Schlüssel 41 der vertrauenswürdigen Instanz 10 sowie ein der Smartcard 40 zugeordnetes asymmetrisches Schlüsselpaar 42 abgespeichert, daß einen öffentlichen und einen privaten Schlüssel der Smartcard 40 umfaßt. Außerdem
- 25 ist auf der Smartcard 40 zumindest ein Programm vorgesehen zur Ver- und Entschlüsselung unter Nutzung des asymmetrischen Schlüsselpaares 42 der Smartcard 40 und zur Verifizierung von mittels des privaten Schlüssels der vertrauenswürdigen Instanz 10 erzeugten Signaturen. Die Verifizierung von Signatu-
- 30 ren erfolgt dabei unter Zuhilfenahme des öffentlichen Schlüssels 41 der vertrauenswürdigen Instanz 10. Darüber hinaus verfügt die Smartcard 40 über einen Zufallszahlengenerator und ist vorzugsweise konform zu IFO 7816/4.
- 35 Am Computer 20 wird eine von der vertrauenswürdigen Instanz 10 erstellte Lizenzinformation 1 bereitgestellt. Die Lizenzinformation 1 umfaßt einen mittels des der Smartcard 40 zuge-

ordneten öffentlichen Schlüssels verschlüsselten Lizenzcode (enc_SC(licencecode)), den der Smartcard 40 zugeordneten öffentlichen Schlüssel (pub_SC) und ein Signatur-Objekt (DS_Object). Das Signatur-Objekt umfaßt nur einen Signaturan-

5 teil eines von der vertrauenswürdigen Instanz 10 signierten Funktionsaufrufs (PSO_DEC - perform security operation mode decrypt) zur Entschlüsselung des Lizenzcodes mittels der Smartcard 40. Des weiteren ist die Lizenzinformation 1 mittels des privaten Schlüssels der vertrauenswürdigen Instanz

10 10 digital signiert (sig_TP), so daß die digitale Signatur der Lizenzinformation 1 im Computer 20 anhand des öffentlichen Schlüssels 21 der vertrauenswürdigen Instanz 10 überprüft werden kann.

15 Zur Realisierung eines Wiederholungsschutzes für den Informations- und Meldungsaustausch zwischen dem Computer 20 und dem Smartcard-Terminal 30 bzw. der Smartcard 40 wird im Computer 20 eine Zufallszahl (rand) erzeugt und diese mittels einer Meldung 2 an die Smartcard 40 übermittelt (give_random). Von

20 der Smartcard 40 wird der Empfang der Zufallszahl durch eine Bestätigungsmeldung 3 quittiert. Nachfolgend wird eine Meldung 4 zur Entschlüsselung des Lizenzcodes vom Computer 20 an die Smartcard 40 übermittelt. Die Meldung 4 zur Entschlüsselung des Lizenzcodes umfaßt eine mittels des privaten Schlüssels der vertrauenswürdigen Instanz 10 digital signierte Angabe einer von der Smartcard 40 auszuführenden Funktion zur

25 Entschlüsselung des Lizenzcodes einschließlich des verschlüsselten Lizenzcodes.

30 Die mittels des privaten Schlüssels der vertrauenswürdigen Instanz 10 digital signierter Angabe der von der Smartcard 40 auszuführenden Funktion zur Entschlüsselung des Lizenzcodes wird im Computer 20 aus dem von der Lizenzinformation 1 umfaßten Signatur-Objekt und dem verschlüsselten Lizenzcode erzeugt. Auf diese Weise wird durch den Computer 20 im Namen

35 der vertrauenswürdigen Instanz 10 ein von der vertrauenswürdigen Instanz 10 signiertes Secure-Messaging-Kommando

(SM_sig_TP) erstellt, wodurch sichergestellt wird, daß die Angabe der von der Smartcard 40 auszuführenden Funktion zur Entschlüsselung des Lizenzcodes und der verschlüsselte Lizenzcode tatsächlich von der vertrauenswürdigen Instanz 10
5 ausgestellt worden sind.

Eine Überprüfung der digitalen Signatur der Angabe der von der Smartcard 40 auszuführenden Funktion durch die Smartcard 40 und einer Ausführung der Funktion zur Entschlüsselung des
10 Lizenzcodes durch die Smartcard 40 bei positiven Überprüfungsergebnis zum Schutz vor Manipulationsversuchen durch Bildung eines gemeinsamen funktionalen Kontextes miteinander verknüpft. Insbesondere ist sichergestellt, daß eine Entschlüsselung des Lizenzcodes nur durch eine dafür vorgesehene
15 Smartcard möglich ist.

Nach Ausführung der Funktion zur Entschlüsselung des Lizenzcodes (perform securitiy operation mode decrypt, angewendet auf den mittels des öffentlichen Schlüssels der Smartcard 40
20 verschlüsselten Lizenzcode) und Entschlüsselung wird der entschlüsselte Lizenzcode unter Anwendung von Secure-Messaging mittels einer Meldung 5 an den Computer 20 übermittelt. Zur Anwendung von Secure-Messaging wird der entschlüsselte Lizenzcode mittels des der Smartcard 40 zugeordneten privaten
25 Schlüssels und der von dem Computer 20 erzeugten Zufallszahl digital signiert (SM_rand_sig_SC). Nach Übermittlung an den Computer 20 wird die digitale Signatur des entschlüsselten Lizenzcodes durch den Computer 20 anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels und der Zufallszahl
30 überprüft. Grundsätzlich wäre es bereits ausreichend, den entschlüsselten Lizenzcode lediglich mittels des der Smartcard 40 zugeordneten Privatschlüssels digital zu signieren und die digitale Signatur anhand des öffentlichen Schlüssels der Smartcard 40 zu überprüfen. Dies würde jedoch einen Verzicht auf den Wiederholschutz bedeuten. Je nach Anwendungsfälle und Sicherheitsanforderungen kann daher eine entsprechende Abwägung angemessener Maßnahmen vorgenommen werden.
35

Nach Überprüfung der digitalen Signatur des entschlüsselten Lizenzcodes wird dieser zumindest temporär zum Zugriff auf die geschützte Software bzw. ein computerbasiertes Objekt bereitgestellt. Um denkbare Manipulationsmöglichkeiten auszuschließen, sollten der entschlüsselte Lizenzcode und ein Überprüfungsprozeßverlauf mit einer jeweiligen Soll-Vorgabe vor Einräumung des Zugriffs auf die geschützte Software abgeglichen werden. Bei erfolgreichem Abgleich kann dann der Zugriff eingeräumt werden.

Die Steuerung des Ablaufs des Verfahrens zur Einräumung eines Zugriffs auf geschützte Software bzw. ein computerbasiertes Objekt ist durch ein Steuerungsprogramm implementiert, daß in einem Arbeitsspeicher des Computers 20 ladbar ist und zumindest ein Codeabschnitt aufweist, bei dessen Ausführung zunächst eine Übermittlung eines mittels eines einer Speicherkarte mit einem Programmcodeprozessor zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode und einer mittels eines privaten Schlüssels einer vertrauenswürdigen Instanz digital signierten Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes an die Speicherkarte veranlaßt wird. Ferner wird bei Ausführung des Codeabschnittes eine Überprüfung der digitalen Signatur der Angabe der von der Speicherkarte auszuführenden Funktion durch die Speicherkarte veranlaßt. Die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion wird dabei anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft. Bei positivem Überprüfungsergebnis werden dann eine Ausführung der Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte und eine Übermittlung eines verschlüsselten Lizenzcodes an den Computer 20 veranlaßt. Schließlich wird bei Ausführung des Codeabschnittes der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt durch den Computer 20 bereitgestellt, wenn das Steuerungsprogramm im Computer 20 abläuft.

Die Anwendung der vorliegenden Erfindung ist nicht auf das hier beschriebene Ausführungsbeispiel beschränkt.

Patentansprüche

1. Verfahren zur Einräumung eines Zugriffs auf ein computerbasiertes Objekt, bei dem
- 5 - eine Speicherkarte mit einem Programmcodeprozessor bereitgestellt wird, auf der zumindest ein der Speicherkarte zugeordneter öffentlicher und privater Schlüssel sowie ein öffentlicher Schlüssel einer vertrauenswürdigen Instanz abgespeichert sind,
 - 10 - eine Lizenzinformation, die zumindest einen mittels des der Speicherkarte zugeordneten öffentlichen Schlüssels verschlüsselten Lizenzcode umfaßt, an einer den Zugriff auf das computerbasierte Objekt steuernden Recheneinrichtung bereitgestellt wird,
 - 15 - der verschlüsselte Lizenzcode und eine mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital signierte Angabe einer von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes an die Speicherkarte übermittelt werden,
 - 20 - die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion überprüft wird,
 - bei positivem Überprüfungsergebnis die Funktion zur Entschlüsselung des Lizenzcodes durch die Speicherkarte ausgeführt und ein entschlüsselter Lizenzcode an die Rechen-
 - 25 - einrichtung übermittelt wird,
 - der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt bereitgestellt wird.
- 30 2. Verfahren nach Anspruch 1, bei dem der öffentliche Schlüssel der vertrauenswürdigen Instanz vor Manipulationen geschützt an der Recheneinrichtung bereitgestellt wird, bei dem die Lizenzinformation mittels eines privaten Schlüssels der vertrauenswürdigen Instanz di-
- 35 gital signiert ist, und bei dem die digitale Signatur der Lizenzinformation in der Recheneinrichtung anhand des öffentli-

chen Schlüssels der vertrauenswürdigen Instanz überprüft wird.

3. Verfahren nach einem der Ansprüche 1 oder 2,
5 bei dem die Lizenzinformation zusätzlich den der Speicherkarte zugeordneten öffentlichen Schlüssel umfaßt, bei dem der entschlüsselte Lizenzcode mittels des der Speicherkarte zugeordneten privaten Schlüssels digital signiert wird, und bei dem die digitale Signatur des entschlüsselten Lizenzcodes in
10 der Recheneinrichtung anhand des der Speicherkarte zugeordneten öffentlichen Schlüssels überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die mittels des privaten Schlüssels der vertrauens-
15 würdigen Instanz digital signierte Angabe der von der Speicherkarte auszuführenden Funktion zur Entschlüsselung des Lizenzcodes in der Recheneinrichtung aus dem verschlüsseltem Lizenzcode und einem Signatur-Objekt erzeugt wird, das nur einen Signaturanteil eines von der vertrauenswürdigen Instanz
20 signierten Funktionsaufrufs zur Entschlüsselung des Lizenzcodes umfaßt.

5. Verfahren nach Anspruch 4,
bei dem die Lizenzinformation zusätzlich das Signatur-Objekt
25 umfaßt.

6. Verfahren nach einem der Ansprüche 1 bis 5,
bei dem der verschlüsselte Lizenzcode und die mittels des privaten Schlüssels der vertrauenswürdigen Instanz digital
30 signierte Angabe der von der Speicherkarte auszuführenden Funktion über eine gesicherte Kommunikationsverbindung von der Recheneinrichtung über eine Leseeinrichtung an die Speicherkarte übermittelt werden.

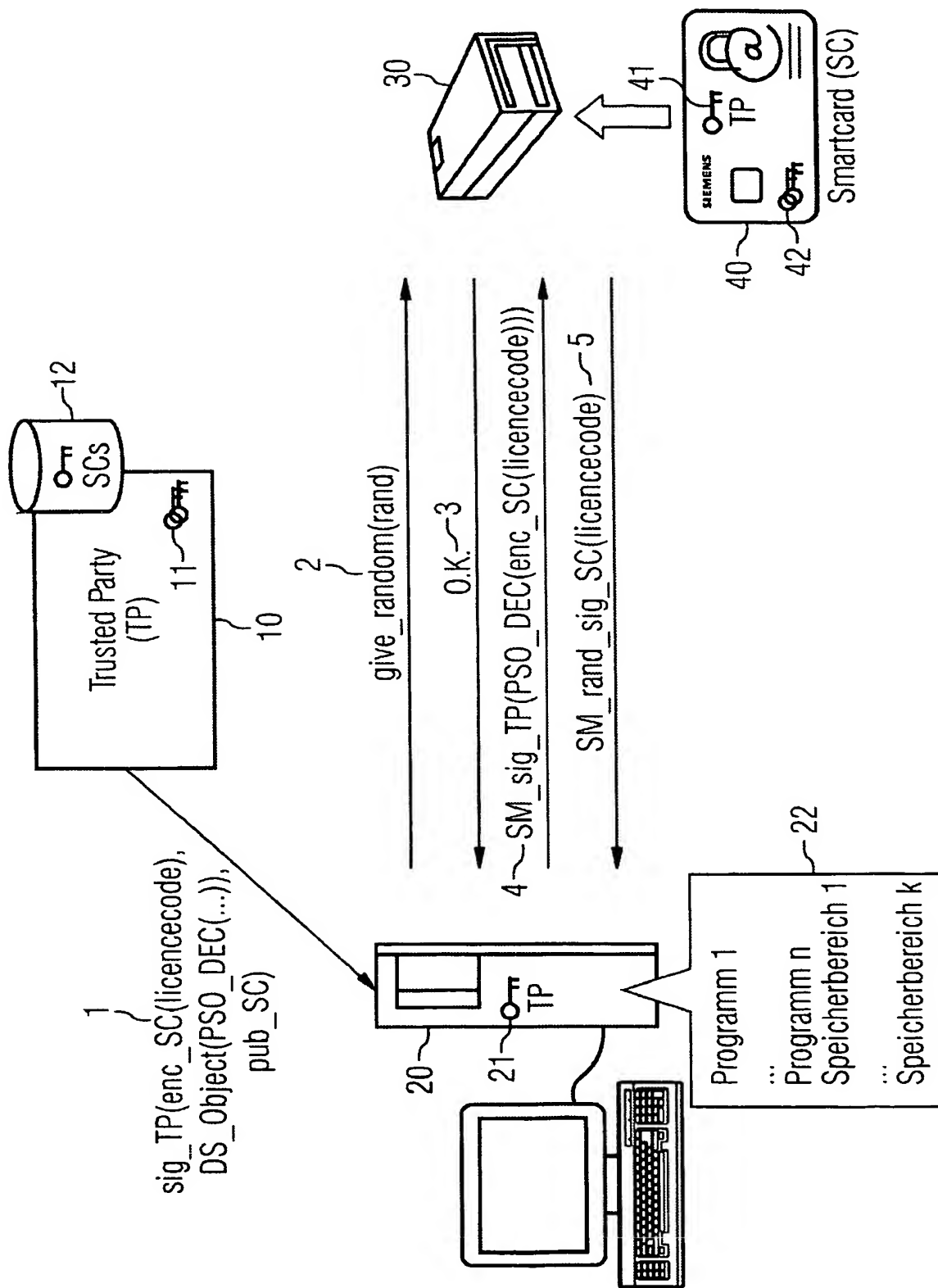
35 7. Verfahren nach einem der Ansprüche 1 bis 6,

bei dem die digitale Signatur der Angabe der von der Speicherkarte auszuführenden Funktion anhand des öffentlichen Schlüssels der vertrauenswürdigen Instanz überprüft wird.

- 5 8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem in der Recheneinrichtung eine Zufallszahl erzeugt und
diese an die Speicherkarte übermittelt wird, bei dem der ent-
schlüsselte Lizenzcode mittels des der Speicherkarte zugeord-
neten privaten Schlüssels und der Zufallszahl digital sig-
10 niert wird, und bei dem die digitale Signatur des entschlüs-
selten Lizenzcodes in der Recheneinrichtung anhand des der
Speicherkarte zugeordneten öffentlichen Schlüssels und der
Zufallszahl überprüft wird.
- 15 9. Verfahren nach einem der Ansprüche 1 bis 8,
bei dem zur Einräumung des Zugriffs auf das computerbasierte
Objekt der entschlüsselte Lizenzcode und ein Überprüfungspro-
zeßverlauf mit einer jeweiligen Soll-Vorgabe abgeglichen wer-
den.
- 20 10. Steuerungsprogramm, das in einen Arbeitsspeicher einer
Recheneinrichtung ladbar ist und zumindest einen Codeab-
schnitt aufweist, bei dessen Ausführung
- eine Übermittlung eines mittels eines einer Speicherkarte
25 mit einem Programmcodeprozessor zugeordneten öffentlichen
Schlüssels verschlüsselten Lizenzcodes und einer mittels
eines privaten Schlüssels einer vertrauenswürdigen Instanz
digital signierten Angabe einer von der Speicherkarte aus-
zuführenden Funktion zur Entschlüsselung des Lizenzcodes
30 an die Speicherkarte veranlaßt wird,
 - eine Überprüfung der digitalen Signatur der Angabe der von
der Speicherkarte auszuführenden Funktion durch die Spei-
cherkarte veranlaßt wird,
 - bei positivem Überprüfungsergebnis eine Ausführung der
35 Funktion zur Entschlüsselung des Lizenzcodes durch die
Speicherkarte und eine Übermittlung eines entschlüsselten
Lizenzcodes an die Recheneinrichtung veranlaßt werden,

- der entschlüsselte Lizenzcode zumindest temporär zum Zugriff auf das computerbasierte Objekt durch die Recheneinrichtung bereitgestellt wird, wenn das Steuerungsprogramm in der Recheneinrichtung abläuft.

1/1



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2004/052244

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|--|-----------------------|
| X | EP 1 076 279 A (HEWLETT PACKARD CO) 14 February 2001 (2001-02-14) paragraphs '0001!', '0008!', '0012!', '0026!', '0027!', '0037!', '0043!', '0046!', '0056!', '0065!' - '0069!' ----- | 1-10 |
| A | EP 0 686 906 A (SUN MICROSYSTEMS INC) 13 December 1995 (1995-12-13) abstract column 4, line 3 - column 5, line 57 ----- | 1-10 |
| A | EP 0 803 789 A (EUROP COMPUTER IND RES) 29 October 1997 (1997-10-29) abstract; figure 2 column 4, line 10 - line 33 column 13, line 50 - column 14, line 58 ----- -/-- | 1-10 |



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O document referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

A document member of the same patent family

Date of the actual completion of the international search

20 December 2004

Date of mailing of the international search report

04/01/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Kerschbaumer, J

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052244

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|------------|---|-----------------------|
| X | US 2003/161473 A1 (FRANSDONK ROBERT W) 28 August 2003 (2003-08-28) paragraphs '0017!, '0076!, '0086! - '0097!, '0299! abstract; figure 16 | 1-10 |
| A | EP 1 055 990 A (HEWLETT PACKARD CO) 29 November 2000 (2000-11-29) abstract paragraphs '0056! - '0058! | 1-10 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2004/052244

| Patent document cited in search report | | Publication date | Patent family member(s) | Publication date |
|---|----|---------------------|----------------------------|---------------------|
| EP 1076279 | A | 14-02-2001 | EP 1076279 A1 | 14-02-2001 |
| | | | DE 60002893 D1 | 26-06-2003 |
| | | | DE 60002893 T2 | 13-05-2004 |
| | | | EP 1203278 A1 | 08-05-2002 |
| | | | EP 1204910 A1 | 15-05-2002 |
| | | | WO 0113198 A1 | 22-02-2001 |
| | | | WO 0113199 A1 | 22-02-2001 |
| | | | JP 2003507784 T | 25-02-2003 |
| | | | JP 2003507785 T | 25-02-2003 |
| EP 0686906 | A | 13-12-1995 | US 5724425 A | 03-03-1998 |
| | | | EP 0686906 A2 | 13-12-1995 |
| | | | JP 8166879 A | 25-06-1996 |
| EP 0803789 | A | 29-10-1997 | AU 716912 B2 | 09-03-2000 |
| | | | AU 1912097 A | 30-10-1997 |
| | | | EP 0803789 A2 | 29-10-1997 |
| | | | US 5935246 A | 10-08-1999 |
| US 2003161473 | A1 | 28-08-2003 | AU 6985601 A | 02-01-2002 |
| | | | EP 1407360 A1 | 14-04-2004 |
| | | | US 2003161476 A1 | 28-08-2003 |
| | | | US 2003165241 A1 | 04-09-2003 |
| | | | US 2003163684 A1 | 28-08-2003 |
| | | | US 2003161335 A1 | 28-08-2003 |
| | | | US 2003167392 A1 | 04-09-2003 |
| | | | WO 0198903 A1 | 27-12-2001 |
| EP 1055990 | A | 29-11-2000 | EP 1055990 A1 | 29-11-2000 |
| | | | EP 1181632 A1 | 27-02-2002 |
| | | | WO 0073880 A1 | 07-12-2000 |
| | | | JP 2003501716 T | 14-01-2003 |

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/052244

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|------------|--|--------------------|
| X | EP 1 076 279 A (HEWLETT PACKARD CO) 14. Februar 2001 (2001-02-14) Absätze '0001!', '0008!', '0012!', '0026!', '0027!', '0037!', '0043!', '0046!', '0056!', '0065!' - '0069!' | 1-10 |
| A | EP 0 686 906 A (SUN MICROSYSTEMS INC) 13. Dezember 1995 (1995-12-13) Zusammenfassung Spalte 4, Zeile 3 - Spalte 5, Zeile 57 | 1-10 |
| A | EP 0 803 789 A (EUROP COMPUTER IND RES) 29. Oktober 1997 (1997-10-29) Zusammenfassung; Abbildung 2 Spalte 4, Zeile 10 - Zeile 33 Spalte 13, Zeile 50 - Spalte 14, Zeile 58 | 1-10 |
| | -/-- | |



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

20. Dezember 2004

Absenddatum des internationalen Recherchenberichts

04/01/2005

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Kerschbaumer, J

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2004/052244

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

| Kategorie* | Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile | Betr. Anspruch Nr. |
|------------|--|--------------------|
| X | US 2003/161473 A1 (FRANSDONK ROBERT W) 28. August 2003 (2003-08-28) Absätze '0017!', '0076!', '0086! - '0097!, '0299! Zusammenfassung; Abbildung 16 ----- | 1-10 |
| A | EP 1 055 990 A (HEWLETT PACKARD CO) 29. November 2000 (2000-11-29) Zusammenfassung Absätze '0056! - '0058! ----- | 1-10 |

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Akenzeichen

PCT/EP2004/052244

| Im Recherchenbericht angeführtes Patentdokument | Datum der Veröffentlichung | Mitglied(er) der Patentfamilie | Datum der Veröffentlichung |
|--|-------------------------------|-----------------------------------|-------------------------------|
| EP 1076279 A | 14-02-2001 | EP 1076279 A1 | 14-02-2001 |
| | | DE 60002893 D1 | 26-06-2003 |
| | | DE 60002893 T2 | 13-05-2004 |
| | | EP 1203278 A1 | 08-05-2002 |
| | | EP 1204910 A1 | 15-05-2002 |
| | | WO 0113198 A1 | 22-02-2001 |
| | | WO 0113199 A1 | 22-02-2001 |
| | | JP 2003507784 T | 25-02-2003 |
| | | JP 2003507785 T | 25-02-2003 |
| EP 0686906 A | 13-12-1995 | US 5724425 A | 03-03-1998 |
| | | EP 0686906 A2 | 13-12-1995 |
| | | JP 8166879 A | 25-06-1996 |
| EP 0803789 A | 29-10-1997 | AU 716912 B2 | 09-03-2000 |
| | | AU 1912097 A | 30-10-1997 |
| | | EP 0803789 A2 | 29-10-1997 |
| | | US 5935246 A | 10-08-1999 |
| US 2003161473 A1 | 28-08-2003 | AU 6985601 A | 02-01-2002 |
| | | EP 1407360 A1 | 14-04-2004 |
| | | US 2003161476 A1 | 28-08-2003 |
| | | US 2003165241 A1 | 04-09-2003 |
| | | US 2003163684 A1 | 28-08-2003 |
| | | US 2003161335 A1 | 28-08-2003 |
| | | US 2003167392 A1 | 04-09-2003 |
| | | WO 0198903 A1 | 27-12-2001 |
| EP 1055990 A | 29-11-2000 | EP 1055990 A1 | 29-11-2000 |
| | | EP 1181632 A1 | 27-02-2002 |
| | | WO 0073880 A1 | 07-12-2000 |
| | | JP 2003501716 T | 14-01-2003 |